# Building PRFs from TPRPs: Beyond the Block and the Tweak Length Bounds

**Wonseok Choi**[1] Jooyoung Lee[2] Yeongmin Lee[2]

Purdue University, West Lafayette, IN, USA

KAIST, Daejeon, Korea

March 27th, 2024

# Outline

# Luby-Rackoff Problem

- Feistel and Coppersmith: designed IBM's Lucifer cipher using Feistel networks
- Luby and Rackoff: analyzed Feistel network when the round function is a secure pseudorandom function (PRF)
  - 3 rounds: a pseudorandom permutation (PRP),
  - 4 rounds: a strong pseudorandom permutation
- Luby-Rackoff problem: how to make secure PRPs from secure PRFs?

# Luby-Rackoff Problem

- Feistel and Coppersmith: designed IBM's Lucifer cipher using Feistel networks

- Luby and Rackoff: analyzed Feistel network when the round function is a secure pseudorandom function (PRF)
  - 3 rounds: a pseudorandom permutation (PRP),
  - 4 rounds: a strong pseudorandom permutation

- Luby-Rackoff problem: how to make secure PRPs from secure PRFs?

# Luby-Rackoff Problem

- Feistel and Coppersmith: designed IBM's Lucifer cipher using Feistel networks
- Luby and Rackoff: analyzed Feistel network when the round function is a secure pseudorandom function (PRF)
  - 3 rounds: a pseudorandom permutation (PRP),
  - 4 rounds: a strong pseudorandom permutation
- Luby-Rackoff problem: how to make secure PRPs from secure PRFs?

# Luby-Rackoff Backward Problem

- A block cipher is typically modeled as a PRP
- Meanwhile, hashes, message authenticate codes (MACs), or authenticated encryptions (AEs) prefer to use PRFs — at least implicitly in their security proofs!
- Luby-Rackoff backward problem: how to make secure PRFs from secure PRPs?

# Luby-Rackoff Backward Problem

- A block cipher is typically modeled as a PRP
- Meanwhile, hashes, message authenticate codes (MACs), or authenticated encryptions (AEs) prefer to use PRFs — at least implicitly in their security proofs!
- Luby-Rackoff backward problem: how to make secure PRFs from secure PRPs?

# Luby-Rackoff Backward Problem

- A block cipher is typically modeled as a PRP
- Meanwhile, hashes, message authenticate codes (MACs), or authenticated encryptions (AEs) prefer to use PRFs — at least implicitly in their security proofs!
- Luby-Rackoff backward problem: how to make secure PRFs from secure PRPs?

# Security of Pseudorandom Function

- $\mathsf{C} : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$: a keyed function
- The advantage of $\mathcal{A}$ in breaking the PRF-security of C

$$\mathbf{Adv}_{\mathsf{C}}^{\mathrm{prf}}(\mathcal{A}) = \Big| \Pr\left[K \leftarrow_{\$} \mathcal{K} : \mathcal{A}^{\mathsf{C}(K,\cdot)} = 1\right] - \Pr\left[\mathsf{F} \leftarrow_{\$} \mathsf{Func}(\mathcal{X}, \mathcal{Y}) : \mathcal{A}^{\mathsf{F}(\cdot)} = 1\right] \Big|$$

- $\mathbf{Adv}_{\mathsf{C}}^{\mathrm{prf}}(q)$: the maximum of $\mathbf{Adv}_{\mathsf{C}}^{\mathrm{prf}}(\mathcal{A})$ over all the distinguishers against C making at most $q$ queries

# Xor of Two Permutations

- How to build secure PRFs from secure PRPs?

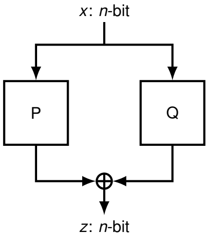


Figure 1: XoP based on two (keyed) PRPs: P and Q

- Those are at most $n$-bit secure

# Xor of Two Permutations

- How to build secure PRFs from secure PRPs?

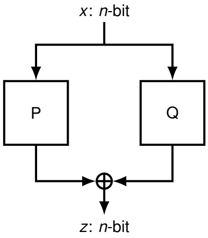


Figure 1: XoP based on two (keyed) PRPs: P and Q

- Those are at most *n*-bit secure

# Tweakable Block Ciphers

- Tweakable block ciphers (TBC) [LRW02] are a generalization of standard block ciphers that accept extra inputs called tweaks

- TWEAK:
  - provides inherent variability to the block cipher
  - makes it easy to design various higher level cryptographic schemes

# Tweakable Block Ciphers

- Tweakable block ciphers (TBC) [LRW02] are a generalization of standard block ciphers that accept extra inputs called tweaks

- TWEAK:
  - provides inherent variability to the block cipher
  - makes it easy to design various higher level cryptographic schemes

# Tweakable Unifrom Random Permutaions

- Keyed TBC should behave like an independent random permutation for each tweak as a tweakable permutation (TPRP)
- The ideal counterpart of a TPRP is called a tweakable uniform random permutation (TURP)

# Tweakable Unifrom Random Permutaions

- Keyed TBC should behave like an independent random permutation for each tweak as a tweakable permutation (TPRP)

- The ideal counterpart of a TPRP is called a tweakable uniform random permutation (TURP)

# How to build PRFs from TPRPs? (1)

- It is easy to achieve $n$-bit PRF security using a TPRP $\tilde{P}$
  - $\tilde{P}(tweak, message) = output$
  - where $n$ is the bit size of message-output space

- By fixing a message and varying tweak inputs, we have an optimally secure PRF, i.e., $F(X) = \tilde{P}(X, C)$
- However, the input domain is limited up to $n$-bit string

- Ideally, a TPRP-based PRF may achieve $(n+t)$-bit security, while taking $(n+t)$-bit inputs (STILL OPEN)

# How to build PRFs from TPRPs? (1)

- It is easy to achieve $n$-bit PRF security using a TPRP $\tilde{P}$
  - $\tilde{P}(tweak, message) = output$
  - where $n$ is the bit size of message-output space

- By fixing a message and varying tweak inputs, we have an optimally secure PRF, i.e., $F(X) = \tilde{P}(X, C)$
- However, the input domain is limited up to $n$-bit string

- Ideally, a TPRP-based PRF may achieve $(n + t)$-bit security, while taking $(n + t)$-bit inputs (STILL OPEN)

# How to build PRFs from TPRPs? (1)

- It is easy to achieve $n$-bit PRF security using a TPRP $\tilde{P}$
  - $\tilde{P}(tweak, message) = output$
  - where $n$ is the bit size of message-output space

- By fixing a message and varying tweak inputs, we have an optimally secure PRF, i.e., $F(X) = \tilde{P}(X, C)$
- However, the input domain is limited up to $n$-bit string

- Ideally, a TPRP-based PRF may achieve $(n + t)$-bit security, while taking $(n + t)$-bit inputs (STILL OPEN)

# How to build PRFs from TPRPs? (2)

- How about using two TPRP $\tilde{P}$, $\tilde{Q}$?

- For simplicity, we only consider $t = n$ here
  - For more general arguments, see our paper!

- We first consider XoP-like construction, which we call MXoP:
  - $\text{MXoP}(X \parallel Y) = \tilde{P}(Y, X) \oplus \tilde{Q}(Y, X)$
  - $X, Y \in \{0, 1\}^n$

- Indeed, this is the same as multiple instances of XoP by regarding $Y$ as a secret key of each instance

- the security can be reduced to that of multi-user PRF security of XoP, i.e., $n$-bit security

# How to build PRFs from TPRPs? (2)

- How about using two TPRP $\tilde{P}$, $\tilde{Q}$?

- For simplicity, we only consider $t = n$ here
  - For more general arguments, see our paper!

- We first consider XoP-like construction, which we call MXoP:
  - $\text{MXoP}(X \parallel Y) = \tilde{P}(Y, X) \oplus \tilde{Q}(Y, X)$
  - $X, Y \in \{0, 1\}^n$

- Indeed, this is the same as multiple instances of XoP by regarding $Y$ as a secret key of each instance

- the security can be reduced to that of multi-user PRF security of XoP, i.e., $n$-bit security

# How to build PRFs from TPRPs? (2)

- How about using two TPRP $\tilde{P}$, $\tilde{Q}$?
- For simplicity, we only consider $t = n$ here
  - For more general arguments, see our paper!
- We first consider XoP-like construction, which we call MXoP:
  - $\mathrm{MXoP}(X \parallel Y) = \tilde{P}(Y, X) \oplus \tilde{Q}(Y, X)$
  - $X, Y \in \{0, 1\}^n$
- Indeed, this is the same as multiple instances of XoP by regarding $Y$ as a secret key of each instance
- the security can be reduced to that of multi-user PRF security of XoP, i.e., $n$-bit security

# How to build PRFs from TPRPs? (2)

- How about using two TPRP $\tilde{P}$, $\tilde{Q}$?
- For simplicity, we only consider $t = n$ here
  - For more general arguments, see our paper!
- We first consider XoP-like construction, which we call MXoP:
  - $\mathrm{MXoP}(X \parallel Y) = \tilde{P}(Y, X) \oplus \tilde{Q}(Y, X)$
  - $X, Y \in \{0, 1\}^n$
- Indeed, this is the same as multiple instances of XoP by regarding $Y$ as a secret key of each instance
- the security can be reduced to that of multi-user PRF security of XoP, i.e., $n$-bit security

# How to build PRFs from TPRPs? (2)

- How about using two TPRP $\tilde{P}$, $\tilde{Q}$?

- For simplicity, we only consider $t = n$ here
  - For more general arguments, see our paper!

- We first consider XoP-like construction, which we call MXoP:
  - $\mathrm{MXoP}(X \parallel Y) = \tilde{P}(Y, X) \oplus \tilde{Q}(Y, X)$
  - $X, Y \in \{0, 1\}^n$

- Indeed, this is the same as multiple instances of XoP by regarding $Y$ as a secret key of each instance

- the security can be reduced to that of multi-user PRF security of XoP, i.e., $n$-bit security

# More on MXoP

- The most recent result from Dinur [Eurocrypt'24], MXoP can be secure up to $2^{3n/2}$ queries, i.e., the adversarial advantage can be bounded by $q/2^{3n/2}$

- Previously, the most tight bound of MXoP was $q^2/2^{2n}$

- By fixing a half of bits of messages, the previous bound is also reduced to $q/2^{3n/2}$, with $3n/2$-bit input space
  - We call this construction $\mathrm{MXoP}_{n/2}$, where $n/2$ indicates we fix $n/2$-bit of messages

# More on MXoP

- The most recent result from Dinur [Eurocrypt'24], MXoP can be secure up to $2^{3n/2}$ queries, i.e., the adversarial advantage can be bounded by $q/2^{3n/2}$
- Previously, the most tight bound of MXoP was $q^2/2^{2n}$
- By fixing a half of bits of messages, the previous bound is also reduced to $q/2^{3n/2}$, with $3n/2$-bit input space
  - We call this construction $\text{MXoP}_{n/2}$, where $n/2$ indicates we fix $n/2$-bit of messages

# More on MXoP

- The most recent result from Dinur [Eurocrypt'24], MXoP can be secure up to $2^{3n/2}$ queries, i.e., the adversarial advantage can be bounded by $q/2^{3n/2}$
- Previously, the most tight bound of MXoP was $q^2/2^{2n}$
- By fixing a half of bits of messages, the previous bound is also reduced to $q/2^{3n/2}$, with $3n/2$-bit input space
  - We call this construction $\text{MXoP}_{n/2}$, where $n/2$ indicates we fix $n/2$-bit of messages

# A New Construction: XoTP

- We propose a new function family to achieve more strong security, dubbed XoTP

- $\text{XoTP}(X \parallel Y) = \tilde{P}(Y, X) \oplus \tilde{Q}(X, Y)$
  - $X, Y \in \{0,1\}^n$

- $\text{XoTP}_c(X \parallel Y \parallel W) = \tilde{P}(W \parallel Y, C \parallel X) \oplus \tilde{Q}(W \parallel X, C \parallel Y)$
  - where $C$ can be any fixed (or not fixed) $c$-bit constant,
  - $X, Y \in \{0,1\}^{n-c}$, and $W \in \{0,1\}^c$

- And yes, $\text{XoTP}_c$ still outperfroms $\text{MXoP}_c$ even together with the recent breakthrough of Dinur!

# A New Construction: XoTP

- We propose a new function family to achieve more strong security, dubbed XoTP
- $\mathrm{XoTP}(X \parallel Y) = \tilde{P}(Y, X) \oplus \tilde{Q}(X, Y)$
  - $X, Y \in \{0,1\}^n$
- $\mathrm{XoTP}_c(X \parallel Y \parallel W) = \tilde{P}(W \parallel Y, C \parallel X) \oplus \tilde{Q}(W \parallel X, C \parallel Y)$
  - where $C$ can be any fixed (or not fixed) $c$-bit constant,
  - $X, Y \in \{0,1\}^{n-c}$, and $W \in \{0,1\}^c$
- And yes, $\mathrm{XoTP}_c$ still outperfroms $\mathrm{MXoP}_c$ even together with the recent breakthrough of Dinur!

# A New Construction: XoTP

- We propose a new function family to achieve more strong security, dubbed XoTP

- $\mathrm{XoTP}(X \parallel Y) = \tilde{P}(Y, X) \oplus \tilde{Q}(X, Y)$
  - $X, Y \in \{0,1\}^n$

- $\mathrm{XoTP}_c(X \parallel Y \parallel W) = \tilde{P}(W \parallel Y, C \parallel X) \oplus \tilde{Q}(W \parallel X, C \parallel Y)$
  - where $C$ can be any fixed (or not fixed) $c$-bit constant,
  - $X, Y \in \{0,1\}^{n-c}$, and $W \in \{0,1\}^c$

- And yes, $\mathrm{XoTP}_c$ still outperfroms $\mathrm{MXoP}_c$ even together with the recent breakthrough of Dinur!

# A New Construction: XoTP

- We propose a new function family to achieve more strong security, dubbed XoTP

- $\mathrm{XoTP}(X \parallel Y) = \tilde{P}(Y, X) \oplus \tilde{Q}(X, Y)$
  - $X, Y \in \{0,1\}^n$

- $\mathrm{XoTP}_c(X \parallel Y \parallel W) = \tilde{P}(W \parallel Y, C \parallel X) \oplus \tilde{Q}(W \parallel X, C \parallel Y)$
  - where $C$ can be any fixed (or not fixed) $c$-bit constant,
  - $X, Y \in \{0,1\}^{n-c}$, and $W \in \{0,1\}^c$

- And yes, $\mathrm{XoTP}_c$ still outperfroms $\mathrm{MXoP}_c$ even together with the recent breakthrough of Dinur!

# Security of XoTP

- The adversarial advantage in breaking the PRF-security of $\mathrm{XoTP}_c$ is upper bounded by

$$O\left(\min\left\{\frac{q}{2^{n+2c}}, \frac{q^2}{2^{3n}}\right\}\right)$$

- In particular, when $c = n/3$, we obtain a $5n/3$-bit to $n$-bit random function which is $5n/3$-bit secure

# Security of XoTP

- The adversarial advantage in breaking the PRF-security of $\mathrm{XoTP}_c$ is upper bounded by

$$O\left(\min\left\{\frac{q}{2^{n+2c}}, \frac{q^2}{2^{3n}}\right\}\right)$$

- In particular, when $c = n/3$, we obtain a $5n/3$-bit to $n$-bit random function which is $5n/3$-bit secure

# Security Comparison

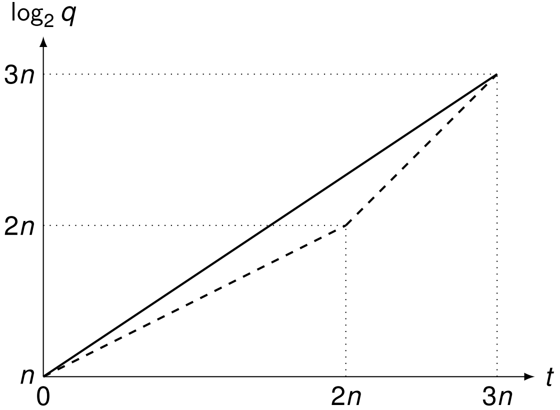


Figure 2: The threshold number of queries $q$ as a function of tweak size $t$. The dashed line is the bound for $\mathrm{MXoP}_{\min\{\frac{t}{2},n\}}$, and the solid line is the bound for $\mathrm{XoTP}_{\frac{t}{3}}$. The graph don't include the recent Dinur's result.

# Mirror Theory

- Lower bound the number of solutions to a system
- $\mathcal{V}_P = \{P_1, \ldots, P_q\}$, $\mathcal{V}_Q = \{Q_1, \ldots, Q_q\}$: unknowns
- $\{z_1, \ldots, z_q\}$: constants

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = z_1, \\ P_2 \oplus Q_2 = z_2, \\ \vdots \\ P_q \oplus Q_q = z_q. \end{cases}$$

- Expected number of solutions (roughly saying): whenever one picks the values of $P_i$ and $Q_i$, $\Pr[P_i \oplus Q_i = z_i] \approx 1/2^n$

$$\frac{\text{\# of choices of } P_i \times \text{\# of choice of } Q_i}{2^{nq}} = \frac{(2^n)_q (2^n)_q}{2^{nq}}$$

# Mirror Theory

- Lower bound the number of solutions to a system
- $\mathcal{V}_P = \{P_1, \ldots, P_q\}, \mathcal{V}_Q = \{Q_1, \ldots, Q_q\}$: unknowns
- $\{z_1, \ldots, z_q\}$: constants

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = z_1, \\ P_2 \oplus Q_2 = z_2, \\ \quad\quad \vdots \\ P_q \oplus Q_q = z_q. \end{cases}$$

- Expected number of solutions (roughly saying): whenever one picks the values of $P_i$ and $Q_i$, $\Pr[P_i \oplus Q_i = z_i] \approx 1/2^n$

$$\frac{\text{\# of choices of } P_i \times \text{\# of choice of } Q_i}{2^{nq}} = \frac{(2^n)_q (2^n)_q}{2^{nq}}$$

# Mirror Theory

- Lower bound the number of solutions to a system
- $\mathcal{V}_P = \{P_1, \ldots, P_q\}$, $\mathcal{V}_Q = \{Q_1, \ldots, Q_q\}$: unknowns
- $\{z_1, \ldots, z_q\}$: constants

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = z_1, \\ P_2 \oplus Q_2 = z_2, \\ \quad\vdots \\ P_q \oplus Q_q = z_q. \end{cases}$$

- Expected number of solutions (roughly saying): whenever one picks the values of $P_i$ and $Q_i$, $\Pr[P_i \oplus Q_i = z_i] \approx 1/2^n$

$$\frac{\#\text{ of choices of } P_i \times \#\text{ of choice of } Q_i}{2^{nq}} = \frac{(2^n)_q (2^n)_q}{2^{nq}}$$

# Graph Representation

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = z_1, \\ P_2 \oplus Q_2 = z_2, \\ \quad\quad \vdots \\ P_q \oplus Q_q = z_q. \end{cases}$$

- can be represented by a simple graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$
  - $\mathcal{V} = \mathcal{V}_P \sqcup \mathcal{V}_Q$
  - $P_i$ and $Q_i$ are connected by a $z_i$-labeled edge for $i = 1, \ldots, q$
  - $\xi_{\max}$: the size of the largest component $(= 2)$

# Example: Graph Representation

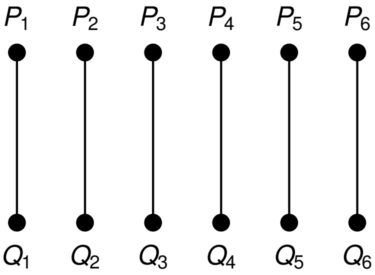


Figure 3: Example: $\xi_{\max} = 2$

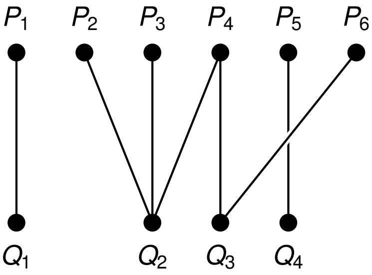


Figure 4: Example: $\xi_{\max} = 6$

# Mirror Theory for $\xi_{max} = 2$ with Relaxed Constraints I

- Variables from TPRPs are not necessarily distinct

- Recall that

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = Z_1 \\ \vdots \\ P_q \oplus Q_q = Z_q \end{cases}$$

- Divide $[q] = \mathcal{P}^{(1)} \sqcup \cdots \sqcup \mathcal{P}^{(a)} = \mathcal{Q}^{(1)} \sqcup \cdots \sqcup \mathcal{Q}^{(b)}$
  - If $P_1, P_2 \in \mathcal{P}^{(1)}$, it implies that $P_1$ and $P_2$ comes from the same tweak (1st tweak), i.e., $P_1 \neq P_2$

# Mirror Theory for $\xi_{max} = 2$ with Relaxed Constraints II

- $i \overset{P}{\sim} j \Leftrightarrow \exists k$ such that $i, j \in \mathcal{P}^{(k)} \Rightarrow P_i \neq P_j$
- $i \overset{Q}{\sim} j \Leftrightarrow \exists k$ such that $i, j \in \mathcal{Q}^{(k)} \Rightarrow Q_i \neq Q_j$
- $h(\Gamma, \overset{P}{\sim}, \overset{Q}{\sim})$: the number of solutions to $\Gamma$ subject to $\overset{P}{\sim}$ and $\overset{Q}{\sim}$
- Let

$$\mathcal{P}_i \overset{\text{def}}{=} \left\{ j < i \,\middle|\, j \overset{P}{\sim} i \right\}, \qquad \mathcal{Q}_i \overset{\text{def}}{=} \left\{ j < i \,\middle|\, j \overset{Q}{\sim} i \right\}$$

# Mirror Theory for $\xi_{max} = 2$ with Relaxed Constraints: Theorem

## Theorem

*Let* $\max_{i\in[a],j\in[b]}\left\{\left|\mathcal{P}^{(i)}\right|,\left|\mathcal{Q}^{(j)}\right|\right\} \leq \frac{2^n}{13}$*. One has*

$$h(\Gamma, \overset{P}{\sim}, \overset{Q}{\sim}) \geq \left(1 - \sum_{i=1}^{q}\left(\frac{2\left|\mathcal{P}_i \cap \mathcal{Q}_i\right|}{2^{2n}} + \frac{20\left|\mathcal{P}_i\right|\left|\mathcal{Q}_i\right|}{2^{3n}}\right) - \frac{6(n+1)^3}{2^{2n}}\right) \times \prod_{i=1}^{q}\left(\frac{(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^n}\right).$$

# History of Mirror Theory

| Publication | Application | $\xi_{\max}$ | $\log q_{\max}$ | Reference |
|---|---|---|---|---|
| eprint 10/287 | XoP | 2 | $n$ | [Pat10] |
| Crypto '18 | DWCDM | 3 | $2n/3$ | [Dat+18] |
| Eurocrypt '19 | CWC+ | Any$^{\dagger}$ | $2n/3$ | [DNT19] |
| JoC '20 | CLRW2 | Any$^{\dagger}$ | $3n/4$ | [JN20] |
| Eurocrypt '20 | DBHtS | Any$^{\ddagger}$ | $3n/4$ | [KLL20] |
| IEEE Trans. IT '22 | XoP | 2 | $n$ | [DNS22] |
| Eurocrypt '23 | Benes | $< 2^{n/4}$ | $n - 2\log \xi_{\max}$ | [Cog+23] |
| – | XoTP1, 2 | 2 | $\gg n$ | This work |

$^{\dagger}$ $q \cdot \xi_{\max} \leq O(2^n)$

$^{\ddagger}$ The number of components of size $\geq 3$ is smaller than $2^{\frac{n}{2}}$

Table 1: History of Mirror theory since [Pat10].

# Application I

- Hash-then-PRF paradigm for constructing MACs
  - a variable-length message is mapped onto a fixed-length value through a hash function,
  - and then a PRF is applied to the hashed message, obtaining a tag
- TBC-based constructions: using two TBC calls at the finalization step
  - PMAC-TBC1k [Nai15], PMACx [LN17]: $n$-bit security
  - ZMAC [Iwa+17]: $\min\left\{n, \frac{n+t}{2}\right\}$-bit security
- $\mathrm{XoTP}_\ell$ combined with a $(t+n-\ell)$-bit hash function $(n < t < 6n)$: provide $\frac{2t+3n}{5}$-bit security with $\ell = \frac{t-n}{5}$

# Application I

- Hash-then-PRF paradigm for constructing MACs
  - a variable-length message is mapped onto a fixed-length value through a hash function,
  - and then a PRF is applied to the hashed message, obtaining a tag
- TBC-based constructions: using two TBC calls at the finalization step
  - PMAC-TBC1k [Nai15], PMACx [LN17]: $n$-bit security
  - ZMAC [Iwa+17]: $\min\left\{n, \frac{n+t}{2}\right\}$-bit security
- XoTP$_\ell$ combined with a $(t+n-\ell)$-bit hash function ($n < t < 6n$): provide $\frac{2t+3n}{5}$-bit security with $\ell = \frac{t-n}{5}$

# Application II

- CTR-type encryption mode with
  - a nonce as a tweak input and
  - a block counter as a block cipher input
- secure up to $\frac{\sigma l}{2^n}$
  - $l$: the maximum message length
  - $\sigma$: the total number of message blocks
- Construct a CTR-type encryption mode of rate $\frac{1}{2}$ from $\mathrm{XoTP}_{\frac{t}{3}}$:
  - $n + \frac{2t}{3}$ bits are available for nonces and counters
  - secure up to $O\left(\frac{\sigma}{2^{n+\frac{2t}{3}}}\right)$
- A numerical example: SKINNY-64-192 (with 128-bit key) $\Rightarrow$ $\mathrm{XoTP}_{21}$: 106-bit input space and security

# Application II

- CTR-type encryption mode with
  - a nonce as a tweak input and
  - a block counter as a block cipher input
- secure up to $\frac{\sigma l}{2^n}$
  - $l$: the maximum message length
  - $\sigma$: the total number of message blocks
- Construct a CTR-type encryption mode of rate $\frac{1}{2}$ from $\mathrm{XoTP}_{\frac{t}{3}}$:
  - $n + \frac{2t}{3}$ bits are available for nonces and counters
  - secure up to $O\left(\frac{\sigma}{2^{n+\frac{2t}{3}}}\right)$
- A numerical example: SKINNY-64-192 (with 128-bit key) $\Rightarrow$ $\mathrm{XoTP}_{21}$: 106-bit input space and security

# Conclusion

## New results

- Beyond the block and the tweak length secure construction: XoTP
- Mirror theory with relaxed contraint

## Future research

- Tight analysis of XoTP
- Propose more constructions (e.g. highly secure encryption scheme even $n$ is small) from a relaxed Mirror theory of $\xi_{\max} > 2$

Thank you for your attention!

# Conclusion

## New results

- Beyond the block and the tweak length secure construction: XoTP
- Mirror theory with relaxed contraint

## Future research

- Tight analysis of XoTP
- Propose more constructions (e.g. highly secure encryption scheme even $n$ is small) from a relaxed Mirror theory of $\xi_{\max} > 2$

Thank you for your attention!

# Conclusion

## New results

- Beyond the block and the tweak length secure construction: XoTP
- Mirror theory with relaxed contraint

## Future research

- Tight analysis of XoTP
- Propose more constructions (e.g. highly secure encryption scheme even $n$ is small) from a relaxed Mirror theory of $\xi_{\mathsf{max}} > 2$

# Thank you for your attention!